negotiation of a related connection within the control connection (as recited in dependent claims 2 and 9). Similarly, the cited prior art fails to teach or suggest the claimed invention embodiments wherein a control connection and the port of a device are both opened using the same process family (as recited in dependent claims 3 and 10).

DEFICIENCIES OF JAIN

Jain merely discloses a firewall configured to identify a dynamical port negotiation relating to an additional File Transfer Protocol (FTP) channel. That firewall includes a classification engine which classifies Protocol Data Units (PDUs) according to the protocol used and performs Network Address Translation (NAT). Thus, Jain merely discloses a conventional method for setting up a related data connection.

However, Jain fails to teach or suggest checking whether a relationship between a port and a device and a control connection fulfills predefined criteria. Further, Jain fails to teach or suggest conditionally blocking such a related connection, if the port of the device does not fulfill the pre-defined criteria. To the contrary, Jain always opens a related connection to a dynamically negotiated port; Jain subsequently denies (i.e., filters) individual PDUs on the opened connection. In this way, Jain treats data traffic according to policies set for the classified PDUs (e.g., FTP or H.225) and performs NAT for the PDUs.

Thus, Jain fails to teach or suggest the claimed invention wherein malicious related connections are detected and blocked by examining relationships between a port negotiated for a related connection and the associated control connection, and by deciding on the basis of this relationship, whether the related connections shall be allowed.

Accordingly, Jain fails to teach or suggest the claimed invention embodiments wherein a port of a device is opened within a predefined time window in relation to noticing negotiation of a related connection within the control connection. Similarly, Jain fails to teach or suggest the claimed invention embodiments wherein a control connection and the port of a device are both opened using the same process family.

Additionally, contrary to the Office Action's assertions, Jain also fails to teach that predetermined criteria require that the control connection and the port of the device are opened by the same process family.

The Office Action asserted that Jain's Fig. 1 illustrates a classification tree. However, the classification tree in Jain's Fig. 1 does not depict processes; rather it depicts protocols. Thus, the tree illustrates how the protocols can be classified. The only process mentioned is the classification process itself, i.e., the process which makes the classification according to

the classification tree. In Jain, a common policy is applied to all PDUs having the same classification, e.g., all FTP protocol PDUs in node 112 are treated with the same policy. As a result, Jain fails to teach or suggest the claimed invention wherein a control connection and a port of the device are opened by the same family, as recited in dependent claims 3 and 10.

The Office Action asserted that Hall remedies the deficiencies of Jain by teaching that a port of a device is opened within a predefined time window in relation to noticing negotiation of a related connection within the control connection (as recited in dependent claims 2 and 9).

DEFICIENCIES OF HALL

However, Hall merely discloses a method and a device for detecting intrusion on a network utilizes a target server running software that is executed for a network client only upon receiving authorization from a monitoring server to execute the software. When an attempt to execute software on the target server by a client is not authorized, Hall's monitoring server notifies the system administrator of the unauthorized attempt.

As illustrated in Fig. 2, for example, there is a connection between the client and the target server. Thus the monitoring server does not monitor the traffic between the client and the target server or control whether a connection to the target server is allowed. Rather, to the contrary, any client (including unauthorized clients) can connect to the target server and execute active software (see, paragraph 30). The target server is configured to ask permission from the monitoring server only if an authorized or unauthorized client attempts to execute the latent software. Thus, Hall fails to remedy the deficiencies of Jain in that Hall also fails to teach or suggest a port of a device is opened within a predefined time window in relation to noticing negotiation of a related connection within the control connection (as recited in dependent claims 2 and 9).

COMBINED TEACHINGS COULD NOT
BE COMBINED TO PROVIDE CLAIMED INVENTION

Moreover, one of ordinary skill in the art could not have combined the teachings of Jain and Hall to provide the claimed invention. Hall's time interval TI-T2 referred to by the Office Action, is not in any way related to a setup of a connection; rather, that time interval determines an administrative period of time for which the client is authorized to use the latent software in the target server. This time may be days, months, or even longer. Therefore,

there is no way that the teachings of Jain and Hall could be combined in a way to render the claimed invention wherein a port of a device is opened within a predefined time window in relation to noticing negotiation of a related connection within the control window, as recited in dependent claims 2 and 9, obvious.

Moreover, the teachings of Hall are not applicable to Jain's firewall, which in situated between a client and a target server to handle processing PDUs. This is because Jain does not relate to software executed on a target server. Accordingly, if one of ordinary skill in the art had applied the teachings of Hall to Jain's system, the result would have merely provided a further monitoring server and a target server configured to ask permission to execute certain software.

CONCLUSION

Accordingly, Applicants submit that claims 1-15 are patentable over the cited prior art because the cited prior art references, analyzed individually or in combination, fail to teach or suggest all the features recited in the rejected claims. Thus, Applicants look forward to receiving a notice indicating the allowability of all the pending claims; however, if anything is necessary to place the application in condition for allowance, Applicants request that the examiner telephone Applicants' representative at the number below.

Please charge any fees associated with the submission of this paper to Deposit Account Number 021010. The Commissioner for Patents is also authorized to credit any over payments to the above-referenced Deposit Account.

Respectfully submitted,

Barnes & Thornburg LLP

By: _____

Christine H. McCarthy
Reg. No. 41,844
Tel. No.: (202) 371-6371
Fax No.: (202) 289-1330

July 12, 2007

Barnes & Thornburg LLP
Suite 900
750 17th Street, N.W.
Washington, D.C. 20006
Tel. No.: (202) 289-1313